<<密码函数的安全性指标分析>>

图书基本信息

书名：<<密码函数的安全性指标分析>>

13位ISBN编号：9787030300089

10位ISBN编号：7030300084

出版时间：2011-2

出版时间：科学出版社

作者：李超　等著

页数：275

<<密码函数的安全性指标分析>>

内容概要

差分均匀度、非线性度、相关免疫阶和代数免疫度分别是刻画密码函数抵抗差分密码攻击、线性密码攻击、相关攻击和代数攻击能力的安全性指标。
《密码函数的安全性指标分析》较为系统地论述了单项安全性指标最优或次优的密码函数的设计与分析，包括完全非线性函数、几乎完全非线性函数、Bent函数、几乎Bem函数和代数免疫度最优的函数的构造、计数和等价性，同时也介绍了非线性度高的弹性函数和代数免疫度最优的函数的构造方法。

本书可以作为密码学专业和信息安全专业高年级本科生和研究生?选修课教材，也可以作为从事密码理论与方法研究的科技人员的参考书。

<<密码函数的安全性指标分析>>

书籍目录

<<密码函数的安全性指标分析>>